REMARKS

Reconsideration and further examination is respectfully requested.

Rejections under 35 U.S.C. §103

Claims 1, 3, 5-12, 18-21, 26-36 and 48-65 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ballardie in view of Bird ("The KryptoKnight Family of Light-Weight Protocol for Authentication and key Distribution...")

Ballardie:

Ballardie proposes a solution to multi-cast key distribution issues, in particular using a Core Based Tree (CBT) protocol. At pages 8-11, Ballardie discloses a group access control mechanism which is illustrated in Figure 1, and includes the steps of a host requesting an authorization stamp from an Authorization Server (AS). The host, upon authorization, receives the Authorization Stamp. The Authorization stamp includes the digital signature *of the AS*. Upon receiving the authorization stamp, the host sends the authorization stamp and an IGMP membership report to the Designated Router (DR). The receiving DR sends a router request to the associated group and an AS in the group responds to the router request. The AS verifies that the digital signature in the authorization stamp matches its own signature (page 9, first paragraph). If it matches, then the DR adds the group to its interface group list.

The present invention is easily distinguished from Ballardie. While Ballardie describes the use of a Certification Authority, which forwards digital signatures of ***a group*** of AS to

connecting hosts for the host to include in join requests, in contrast the present invention provides an authentication key ***which is unique to the particular host*** that seeks to join the shared tree. The unique authentication key is also forwarded to the rendezvous point which forms the root of the tree. While Ballardie's AS compares an authorization stamp ***which is provided to a plurality of hosts*** against *its own* digital signature, the rendezvous point of the present invention *compares the unique authentication key for the host against a previously stored authentication key* ***associated with the host*** *to validate the particular host*. The authentication system of Ballardie does not include such capabilities of unique host validation; rather, as described in Ballardie, Ballardie authenticates on a general sub-net level. Therefore, Ballardie neither describes nor suggests the claimed step of "...the host device forwards an authentication key, uniquely generated by a key server for the host device, to the designated device..."

The Examiner, in the office action, never addresses the particular limitation of the claims, that the authentication key is *uniquely generated by a key server for the host device*. It appears that the Examiner has not given patentable weight to this limitation for some reason which is unclear to the Applicant. Accordingly, for at least the reason that the combination of references fails to teach such a limitation, the rejection is overcome, and should be withdrawn.

Applicants note that the Examiner relies on Bird as teaching a two way authentication with tag field. The Examiner states:

"... Bird discloses a protocols for performing a two way authentication with tag field ... and a nonce field ..." Applicant notes that in the previous office action, Applicant had removed the language of the nonce field from the claims, and for some reason that is not apparent to the Applicant, the Examiner is referring to old claim language.

Bird describes a family of light-weight authentication and key distribution protocols suitable for use in the low layer of network architectures. (Abstract, Bird).

The Examiner relies on page 32, second column, paragraph 2 as teaching several elements of the claims. This portion of Bird describes:

"... One of the protocols ... is represented in Fig. 1. In this figure, the letters A and B stand for the identifiers of two network entities performing two-way authentication. The variables Na and Nb are one-time random numbers (called nonces) used by each party to callenge the other to prove its identity. The notations MACab and MACba denote cryptographic one-way hash functions, called Message Authentication Codes, computed with keys Kba and Kab respectively, and used to guarantee the authenticity of their parameter string. ... Implementing the MAC functions with a symmetric cryptographic system such as DES [8] Kab and Kba are (typically equal) length secret keys shared by A and B..."

Although Bird describes that there are secret keys shared by A and B, there is no mention or suggestion of one key that is uniquely generated for the host. Thus, even if Bird does teach what the Examiner suggests, it has little to do with the language of the claims, which states "...wherein the encoded join request comprises a tag field computed using a keyed hashed function and the authentication key..." and wherein the authentication key is uniquely generated for the host device. Bird thus does nothing to overcome the inadequacies of Ballardie in this regard.

The Examiner states, at page 4, that Mittra further discloses the rendezvous point device is a root of a shared tree and authenticates the encoded join request by comparing the authentication key received in the tag against a stored authentication key associated with the host device.

Applicant would submit that such a statement ignores the hierarchical delegation of authority endorsed by Mittra. For example, Mittra describes, at page 282:

"... Upon receiving a JOIN request, the GSA checks it database and decide whether to approve or deny the request. Assuming the request is approved, it (1) generates a secret (Kgsa-mbr)... to be shared only with the new member, (2) stores the secret along with any other relevant information concerning the new member in a private database... and (3) communicates Kgsa-mbr to the new member using the secure channel...

... the GSA now needs to chage Ksgrp and make Ksgrp known to the current members of the subgroup and the joining member. To do this, the GSA mulitcasts a GRP_KEY_UPDATE message contining K'sgrp ... to the current multicast group.

... of course, in order to process the JOIN, the GSA (if it is itself a GSI) must itself be part of the secure multicast group. If it is not, then it needs to follow a similar procedure to join its parent subgroup. *The only difference between the JOIN of a GSI as opposed to that of a sender or receiver is that the GSI is also supplied .. an ACL or other database that it can use to process JOINS of its own..."*

One difference between the claimed invention and Mittra involves the use of *the designate device* to encode the join request, using the provided key. In addition, in Mittra, it is noted that the JOIN request itself does not have any key associated with it; rather, the appropriateness of the JOIN request is determined via examination of an ACL. The key of Mittra therefore is not generated until after the ACL is approved.

In order to properly support a rejection under 35 U.S.C. §103, it is noted that prior art must teach the limitations *as claimed* in order to support a rejection. While Ballardie teaches a tree joining process is secure, it is clear that the method used is fundamentally different from the claimed invention. As described above, Ballardie distributes the AS digital signature to hosts, and performs a comparison of the AS digital signature at the AS when the membership report is

received from the DR. While Ballardie mentions the word 'key' it is also clear that authentication keys are not used in the manner claimed by Ballardie. In fact it is noted that Ballardie states, at page 6 "...

When combining Ballardie and Mittra, the Examiner must resolve the differences in the particularly inventions, and weigh any statements in the references that would tend to teach away from the suggested modification. Although the Examiner concludes that Mittra teaches that it would be desirable to use an authentication key for each host, the system of Ballardie which includes the addition indirectness of designated routers, clearly states at page 6that "... It is possible to use a separate SAID for each sender of multicast traffic, but this has serious scaling drawbacks..." Applicants would respectfully submit that such language teaches away from a system such as that claimed. It is well known that the test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art, and all teachings in the prior art must be considered to the extent that they are in analogous arts. Where the teachings of two or more prior art references conflict, the examiner must weigh the power of each reference to suggest solutions to one of ordinary skill in the art, considering the degree to which one reference might accurately discredit another. *In re Young*, 927 F.2d 588, 18 USPQ2d 1089 (Fed. Cir. 1991). The language of Ballardie is evidence that teaches away from the modifications must be considered by the Examiner, and for at least this reason the combination of references is improper.

However, even if the references could be combined, it is unclear to the Applicant how the limitations of the claims which deal with encoding of the JOIN request being performed by the designated device is taught or suggested by the references.

Accordingly, for at least the reason that the combination of references fails to describe or suggest several elements of the claim 1, and further because Ballardie essentially teaches away from the invention as claimed, it is respectfully requested that the rejection be withdrawn.

Independent claims 20, 22, 29, 32, 48, 53, 58 and 65

Each of the independent claims recites that the authentication key is uniquely associated with the host device, that the designated device performs the encoding and further detail that the rendezvous point authenticates the host device by comparing the unique authentication key against a stored key associated with the host device. No such structure is shown or suggested by Ballardie, Bird or Mittra, either alone or in combination. " Accordingly, for at least this reason Applicant submits that the independent claims are patentably distinct over the references. In addition, their respective dependent claims are patentable for at least the same reasons as their parent independent claims.

Conclusion:

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone the undersigned, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully submitted,

__December 28, 2007___
Date

___/Lindsay G. McGuinness/_____
Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park
Acton, MA 01720
(978) 264-6664

Docket No. 120-244
Dd: 11/26/2007